REMARKS

In response to the Non-Final Office Action dated May 31, 2007, Applicants respectfully request reconsideration. Claims 1-17 were previously pending in this application. By this paper, claim 3 has been amended. No claims have been added or amended. As a result, claims 1-17 are pending for examination with claims 1, 3, 8, and 10 being independent claims. No new matter has been added.

I. Summary of Telephone Conference with Examiner

First, Applicants' representatives appreciate the courtesies extended by Examiner Lemma in granting and conducting a telephone conference on August 15, 2007. Applicants were represented at the interview by Joseph Teja and Technology Specialist Andrew Tibbetts. During the telephone conference, Applicants' representatives presented to the Examiner a general overview of Applicants' invention as recited in the claims. The rejections under §112 were discussed, with Applicants pointing out to the Examiner the language in the specification providing support for the claims as pending. The cited Snell reference was also discussed.

During that discussion, the Examiner agreed that the claims as pending are supported by the specification and distinguish the combination of Applicants' Admitted Prior Art and the Snell reference. The Examiner also indicated that the combined subject matter contained in dependent claim 3 and independent claim 1 appeared to be allowable. Accordingly, Applicants have rewritten claim 3 in independent claim to incorporate all limitations of claim 1.

Further details of various topics discussed during the telephone conference with the Examiner are included in the remarks below.

II. Claim Rejections under 35 U.S.C. §112

Claims 1-17 were rejected under 35 U.S.C. 112, first paragraph. As indicated above, the Examiner acknowledged during the telephone conference that support for the claim language at issue may be found, for example, at page 8, lines 28-30, of the specification as pending: "According to the present invention, a substitution box is masked by another random value, the bytes of which (or more generally, the blocks of a size corresponding to the size of the blocks of the code taken into account in the substitution box) are all identical."

Accordingly, the Examiner agreed to withdraw the rejection of claims 1-17 under 35 U.S.C. §112.

III. Claim Rejections Under 35 U.S.C. §103

Claims 1-17 stand rejected under 35 U.S.C. 103(a) as allegedly being obvious over Applicants' Admitted Prior Art ("AAPA") in view Published U.S. Patent Application No. 2003/0223580 ("Snell"). Applicants respectfully traverse these rejections.

As discussed above, the Examiner acknowledged that combination of AAPA and Snell does not teach or suggest all limitations of the pending claims. For example, referring to claim 1, neither the AAPA nor Snell—or any combination thereof—teaches or suggests a cyphering/decyphering method "wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical."

More specifically, there is no teaching to be found in either Snell or the admitted prior art of the exact contents of the random numbers. The Office Action asserts on page 4 that this limitation is taught in Applicants' admission of prior art, but the methods describe in the background of the instant application do not disclose any such requirement. Both the admitted prior art and Snell simply disclose generating random numbers of a necessary length—Snell going one step further, requiring that the length of the random number equal that of the data to be ciphered—but neither reference discloses that the contents of the random number be limited to one in which all the blocks of bits are identical. Since claim 1 does recite the random number being comprised of a plurality of blocks of bits, and wherein each block of bits is identical, neither the admitted prior art nor Snell, alone or in combination, teaches or suggests all elements of claim 1.

Each of the other independent claims (i.e., claims 3, 8, and 10) include limitations that similarly distinguish over any combination of AAPA and Snell. For example:

independent claim 3 recites, *inter alia*, a cyphering/decyphering method "wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical;"

independent claim 8 recites, *inter alia*, an integrated circuit for cyphering/decyphering "wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical;" and

independent claim 10 recites, *inter alia*, a method "wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical."

In view of the foregoing, it is clear that no *prima facie* case of obviousness has been established, as there is no teaching or suggestion in the prior art of record that satisfies all the limitations of the pending claims. Therefore, it is respectfully requested that the rejection of claims 1-17 under §103 as purportedly being obvious over AAPA in view of Snell be withdrawn.

Again, Applicants respectfully point out that, with respect to claim 3 as amended herein, the Examiner has indicated preliminarily that the claim as amended appears to be in allowable condition.

CONCLUSION

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment set forth in the Office Action does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Furthermore, nothing in this paper should be construed as intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify any concession of unpatentability of the claim prior to its amendment.

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicants' representative at the telephone number indicated below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,

Dated: September 25, 2007

By: _____

Joseph Teja, Jr.
Registration No.: 45,157
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
(617) 646-8000